Raytheon

ECS Project

Engineering Technical Directive **No. 01-015**

Subject: CGI-BIN programs can be used to execute commands using HTTP shell interpreter **7 November 2001**

The following directive is issued to the PVC and VATC.

Issue: A common Web server misconfiguration is to put shell interpreters (such as sh, csh, etc.) in the cgi-bin directory. Also, some early Web server documentation stated that CGI script interpreters (such as Perl, Tcl, etc.) should be placed in the cgi-bin directory.

Placement of shell interpreters and CGI script interpreters in the cgi-bin directory could allow remote users to execute commands through the interpreters. By sending specially formatted HTTP requests, an attacker could cause these shells to execute commands. For example, an attacker could send a specially formatted HTTP request that would cause password files to be emailed.

Fix: 1. Determine if any cgi-bin programs rely on shell interpreter access. If they do, move the shell interpreter outside the www root, and modify the cgi-bin programs to look for the shell interpreter in the new location. If no programs use the shell interpreter, remove it from the cgi-bin directory for the following Hosts:

VATC
198.118.232.24

Testing: Evaluate locally authored CGI executables to ensure that they do not pass unvalidated user-supplied data to system commands.

Implementation: Execute the procedure listed in the **Fix:** section above.

Point of Contact: Mel Hudson, tele: 301/925-1099, email: mhudson@eos.east.hitc.com

Approved By: V. Maclin
Director, Systems Engineering

Reference CCR: 01-0860

--------End of Directive-------